

a copy of the clause(s), justification for its use, and evidence of legal counsel review to the CPO in accordance with (HSAR) 48 CFR 3001.304 for possible inclusion in the HSAR.

(B) Provisions and clauses used on a one-time basis (i.e., non-standard provisions and clauses) may be approved by the contracting officer, unless a higher level is designated by the Component. This authority is subject to:

(1) Evidence of legal counsel review in the contract file;

(2) Inserting these clauses in the appropriate sections of the uniform contract format; and

(3) Ensuring the provisions and clauses do not deviate from the requirements of the FAR and HSAR.

[68 FR 67871, Dec. 4, 2003, as amended at 71 FR 48802, Aug. 22, 2006]

Subpart 3052.2—Text of Provisions and Clauses

3052.204-70 Security requirements for unclassified information technology resources.

As prescribed in (HSAR) 48 CFR 3004.470-3, insert a clause substantially the same as follows:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within ____ ["insert number of days"] days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

[71 FR 25772, May 2, 2006]

3052.204-71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as follows with appropriate alternates: